Y. KOMATSU
Filed 8-7-03
1 of 1

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年 ８月 ８日

出 願 番 号
Application Number: 特願２００２－２３１８０６

[ST. 10/C]: [ＪＰ２００２－２３１８０６]

出 願 人
Applicant(s): ＮＥＣビューテクノロジー株式会社

２００３年 ７月２８日

特許庁長官
Commissioner,
Japan Patent Office 今 井 康 夫

出証番号 出証特２００３－３０５９５３８

【書類名】　特許願

【整理番号】　21110140

【提出日】　平成14年 8月 8日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 11/30

G06F 15/00

【発明者】

【住所又は居所】　東京都港区芝五丁目３７番８号

エヌイーシービューテクノロジー株式会社内

【氏名】　小松　義治

【特許出願人】

【識別番号】　300016765

【住所又は居所】　東京都港区芝五丁目３７番８号

【氏名又は名称】　エヌイーシービューテクノロジー株式会社

【代理人】

【識別番号】　100084250

【弁理士】

【氏名又は名称】　丸山　隆夫

【電話番号】　03-3590-8902

【手数料の表示】

【予納台帳番号】　007250

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0008450

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子機器及びその不正使用防止方法並びにその不正使用防止プログラム

【特許請求の範囲】

【請求項１】　自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、

外部装置を接続するためのインタフェースと、

該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記機能制限と所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、

該暗証キーを記憶する記憶手段と、

前記インタフェースを介して接続されている外部装置から取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する判断手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器。

【請求項２】　自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、

外部装置を接続するためのインタフェースと、

該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、

該暗証キーを記憶する記憶手段と、

前記インタフェースを介して接続されている外部装置から取得した装置特定情報が、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能

制限のうち前記装置特定情報と関連する機能制限を解除する制限解除手段とを有する電子機器。

【請求項３】　自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする手段と、

該暗証キーを記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器。

【請求項４】　自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、

該暗証キーを少なくとも一つ記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、前記記憶手段に記憶されている暗証キーの装置特定情及び接続経路情報と一致するか否かを判断する判断手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器。

【請求項５】　自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけた情報を暗証キーとする手段と、

該暗証キーを少なくとも一つ記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限のうち前記装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器。

【請求項６】　自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、

該暗証キーを少なくとも一つ記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、前記記憶手段に記憶されているいずれかの暗証キーと一致するか否かを判断する判断手段と

、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限のうち前記装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器。

【請求項７】　前記外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる手段をさらに有することを特徴とする請求項１から６のいずれか１項記載の電子機器。

【請求項８】　前記判断手段が判断を行ってから所定の時間が経過した後に、前記機能制限を再設定する手段をさらに有することを特徴とする請求項１から７のいずれか１項記載の電子機器。

【請求項９】　外部装置を接続するためのインタフェースを備えた電子機器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記機能制限と前記第１の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

前記インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否か判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項１０】　外部装置を接続するためのインタフェースを備えた電子機

器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースを介して接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限のうち、前記第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項１１】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する記憶工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から装

置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報の組み合わせが、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項１２】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記外部装置が、前記第１の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを組にした情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、

前記外部装置が、前記第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報と、前記第２の接続経路情報との対が、前記記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において

設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項１３】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用防止方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記各機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、

判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限のうち、前記第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行することを特徴とする電子機器の不正使用防止方法。

【請求項１４】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正利用防止方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記外部装置が、前記第１の装置特定情報取得工程においていずれのインタフ

ェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する第１の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、

前記外部装置が、前記第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報及びこれに関する第２の接続経路情報との対が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続経路情報の対と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限のうち前記第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項１５】　前記第１の装置特定情報取得工程の後段に、前記第１の装置特定情報取得工程において前記電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程をさらに有することを特徴とする請求項９から１４のいずれか１項記載の電子機器の不正使用防止方法。

【請求項１６】　前記判断工程の実行後所定の時間が経過した時点で、前記機能制限を再設定する工程をさらに有することを特徴とする請求項９から１５のいずれか１項記載の電子機器の不正使用防止方法。

【請求項１７】　外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能

制限を設定する機能制限工程と、

前記インタフェースを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記機能制限と前記第１の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

インタフェースを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否か判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項１８】　外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器の機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースを介して前記電子機器に接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において

設定した機能制限のうち、前記第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項１９】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する記憶工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報の組み合わせが、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項２０】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記外部装置が、前記第１の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経

路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、

前記外部装置が、前記第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報と、前記第２の接続経路情報との対が、前記記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項２１】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶させる工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、

判断工程において一致すると判断した場合に、前記機能制限工程において設定

した機能制限のうち、前記第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項２２】　外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、

前記外部装置が、前記第１の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する第１の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、

該暗証キーを少なくとも一つ記憶手段に記憶させる工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、

前記外部装置が、前記第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、

前記第２の装置特定情報取得工程において取得した装置特定情報及びこれに関する第２の接続経路情報との対が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続経路情報の対と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限のうち前記第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特

徴とする電子機器の不正使用防止プログラム。

【請求項２３】　前記電子機器を制御する実質的なコンピュータに、前記第１の装置特定情報取得工程において前記電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程を、前記第１の装置特定情報取得工程の後段においてさらに実行させることを特徴とする請求項１６から２２のいずれか１項記載の電子機器の不正使用防止プログラム。

【請求項２４】　前記電子機器を制御する実質的なコンピュータに、前記判断工程の実行後所定の時間が経過した時点で、前記機能制限を再設定する工程をさらに実行させることを特徴とする請求項１６から２３のいずれか１項記載の電子機器の不正使用防止プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、使用権限のない者の不正な使用を防止した電子機器及び電子機器の不正な利用を防止する方法及びそのプログラムに関し、特に、接続された外部装置を物理的な鍵として不正な使用を防止する電子機器及びその不正使用防止方法並びにその不正使用防止プログラムに関する。

【０００２】

【従来の技術】

従来、電子機器を不特定多数人が使用可能な環境に設置する場合には、盗難や情報の盗用を防止するための対策を施す必要があった。

【０００３】

例えば、電子機器自体の盗難を防止するために、電子機器をワイヤやチェーン等で机などに固定し、電子機器を設置位置から所定範囲内でしか移動できないようにすることがある。

【０００４】

また、情報の盗用を防止するために、電子機器にパスワードを設定して、パスワードを知らない者が電子機器を利用できないようにすることがある。同様の目

的で、ユーザ認証用の装置（例えば、カードリーダ）を接続又は内蔵したりして、情報の盗用を防止することもある。

【０００５】

しかし、電子機器をワイヤなどを用いて固定していても、ワイヤやチェーンを切断すれば電子機器を盗むことはできてしまう。また、電子装置の筐体にワイヤやチェーンなどを取り付けるための構造を設けなければならないため、装置の外観をデザインする上で制約を受けることとなる。

【０００６】

また、電子機器にパスワードを設定した場合でも、例えば“over　shoulder crack”（パスワードの盗み見）などによってパスワードが漏洩してしまうと、本来情報に対してアクセスする権限がない利用者が情報に不正にアクセスし盗用することができてしまう。

【０００７】

さらに、情報の盗用を試みようとする者は、時間さえ十分にあればブルートフォースアタック（総当たり攻撃）によってパスワードを解読してしまうことも可能である。

パスワードを設定する者が十分な知識を備えていれば、他人に解読されにくいパスワードを設定することも可能ではある。しかし、他人に解読されにくいパスワードとはすなわち桁数が多く複雑なパスワードであるため、電子機器に関する知識に乏しい者にとっては利用しやすいものではない。例えば、パスワードの設定者自身がパスワードを忘れてしまい、電子機器を利用できなくなる可能性がある。

【０００８】

加えて、電子機器にカードリーダなどのユーザ認証用の装置を接続又は内蔵することは、電子機器自体やこれを適用したシステムの価格の上昇を招くことになる。加えて、ＰＤＡを適用した小規模なシステムにおいては、システムにユーザ認証用の装置を組み込むことが難しいこともある。

【０００９】

このように、従来は、電子機器の盗難や情報の盗用を防止するために十分な対

策が取られているとはいえなかった。

【００１０】

コンピュータシステムにおけるセキュリティーの向上を目的とした従来技術として、特開平１０－４９４９３号公報に開示される「コンピュータシステム」がある。

このコンピュータシステムでは、コンピュータ本体及び周辺装置に識別番号を登録するための不揮発メモリがそれぞれ搭載されている。コンピュータ本体に周辺機器が接続されると、コンピュータ本体は、接続された周辺機器から登録番号を取得し、コンピュータ本体の登録番号と一致するか否かを判断し、コンピュータ本体の登録番号と一致する周辺機器のみを使用可能とするものである。

【００１１】

【発明が解決しようとする課題】

しかしながら、上記公報のコンピュータシステムは、コンピュータ本体に接続される周辺機器の盗難を防止することを目的としたものである。換言すると、上記公報のコンピュータシステムは、コンピュータ本体と登録番号が一致しない周辺機器を使用不可能とするものである。すなわち、このコンピュータシステムは、コンピュータ本体を盗まれないようにしたり、情報の盗用を防ぐことを目的としてはいなかった。

【００１２】

本発明は係る問題に鑑みてなされたものであり、不特定多数人が利用可能な環境に設置される電子機器の盗難を防止するとともに、電子機器に記憶された情報が盗用されることを防止する電子機器及びその不正使用防止方法並びにその不正使用防止プログラムを提供することを目的とする。

【００１３】

【課題を解決するための手段】

上記目的を達成するため、本発明は、第１の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、外部装置を接続するためのインタフェースと、該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、機

能制限と所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、該暗証キーを記憶する記憶手段と、インタフェースを介して接続されている外部装置から取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

【００１４】

また、上記目的を達成するため、本発明は、第２の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、外部装置を接続するためのインタフェースと、該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、該暗証キーを記憶する記憶手段と、インタフェースを介して接続されている外部装置から取得した装置特定情報が、記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限のうち装置特定情報と関連する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

【００１５】

また、上記目的を達成するため、本発明は、第３の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする手段と、該暗証キーを記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器を提供するも

のである。

【００１６】

また、上記目的を達成するため、本発明は、第４の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、該暗証キーを少なくとも一つ記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、記憶手段に記憶されている暗証キーの装置特定情及び接続経路情報と一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

【００１７】

また、上記目的を達成するため、本発明は、第５の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけた情報を暗証キーとする手段と、該暗証キーを少なくとも一つ記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限のうち装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

【００１８】

また、上記目的を達成するため、本発明は、第６の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、該暗証キーを少なくとも一つ記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、記憶手段に記憶されているいずれかの暗証キーと一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限のうち装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

【００１９】

上記本発明の第１から第６のいずれの態様において、外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる手段をさらに有することが好ましい。また、判断手段が判断を行ってから所定の時間が経過した後に、機能制限を再設定する手段をさらに有することが好ましい。

【００２０】

また、上記目的を達成するため、本発明は、第７の態様として、外部装置を接続するためのインタフェースを備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、機能制限と第１の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、イン

タフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否か判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

【００２１】

また、上記目的を達成するため、本発明は、第８の態様として、外部装置を接続するためのインタフェースを備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースを介して接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

【００２２】

また、上記目的を達成するため、本発明は、第９の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、機能制限と、一つ以上の特定の装置特定

情報の組み合わせとを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する記憶工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報の組み合わせが、記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

【００２３】

また、上記目的を達成するため、本発明は、第１０の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、外部装置が、第１の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを組にした情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、外部装置が、第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、第２の装置特定情報取得工程において取得した装置特定情報と、第２の接続経路情報との対が、記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

【００２４】

また、上記目的を達成するため、本発明は、第１１の態様として、外部装置を

接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用防止方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、各機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行することを特徴とする電子機器の不正使用防止方法を提供するものである。

【００２５】

また、上記目的を達成するため、本発明は、第１２の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正利用防止方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、外部装置が、第１の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する第１の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、外部装置が、第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、第２の装置特定情報

取得工程において取得した装置特定情報及びこれに関する第２の接続経路情報との対が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続経路情報の対と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限のうち第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

【００２６】

上記本発明の第７から第１２の態様においては、第１の装置特定情報取得工程の後段に、第１の装置特定情報取得工程において電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程をさらに有することが好ましい。また、判断工程の実行後所定の時間が経過した時点で、機能制限を再設定する工程をさらに有することが好ましい。

【００２７】

また、上記目的を達成するため、本発明は、第１３の態様として、外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、機能制限と第１の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、インタフェースを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否か判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

【００２８】

また、上記目的を達成するため、本発明は、第１４の態様として、外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器の機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースを介して電子機器に接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

【００２９】

また、上記目的を達成するため、本発明は、第１５の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する記憶工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報の組み合わせが、記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、判断工

程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

【００３０】

また、上記目的を達成するため、本発明は、第１６の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、外部装置が、第１の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から装置特定情報を取得する第２の装置特定情報取得工程と、外部装置が、第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、第２の装置特定情報取得工程において取得した装置特定情報と、第２の接続経路情報との対が、記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

【００３１】

また、上記目的を達成するため、本発明は、第１７の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から該

装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶させる工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、第２の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

【００３２】

また、上記目的を達成するため、本発明は、第１８の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第１の装置特定情報取得工程と、外部装置が、第１の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第１の接続経路情報を生成する第１の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する第１の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、該暗証キーを少なくとも一つ記憶手段に記憶させる工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第２の装置特定情報取得工程と、外部装置が、第２の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第２の接続経路情報を生成する第２の接続経路情報生成工程と、第２の装置特定情報取得工程において取得した装置特定情報及びこれに関する第２の接続経路情報との対が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続

経路情報の対と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限のうち第２の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

【００３３】

上記本発明の第１３から第１８のいずれかの態様においては、電子機器を制御する実質的なコンピュータに、第１の装置特定情報取得工程において電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程を、第１の装置特定情報取得工程の後段においてさらに実行させることが好ましい。また、電子機器を制御する実質的なコンピュータに、判断工程の実行後所定の時間が経過した時点で、機能制限を再設定する工程をさらに実行させることが好ましい。

【００３４】

【発明の実施の形態】

〔発明の概要〕

図１を用いて、本発明の概要を説明する。本発明を適用した電子機器は、その機能の少なくとも一部に制限が設定されており、制限が設定されている機能については、その制限を解除しない限り使用不能となっている。機能制限の例としては、例えば、電子機器としての機能が全く使用できなくするものであっても良いし、特定の動作（例えば、特定の情報に対するアクセス）のみが使用できなくするものであっても良い。

【００３５】

また、本発明を適用した電子機器は、インタフェースを介して接続された外部装置をユニークに又はそれに準じて特定する機能（例えば、ＣＩＳタプルやシリアル番号を外部装置から取得する機能など）を備えている。例えば、接続された外部装置に自装置をユニークに特定する情報（ＭＡＣアドレスやシリアル番号など）が登録されている場合は、この情報を外部装置から取得することで、接続された外部装置をユニークに特定できる。また、接続された外部装置に自装置をユ

ニークに示す情報が登録されていない場合は、この装置に登録されている製造元や製品の名称を示す情報を取得することで、この装置を製品レベルや製造元レベルで特定できる。これらの情報は、既存の外部装置に予め登録されているものであり、本発明を実現するために特別な情報を外部装置に記録させておく必要はない。

さらに、外部装置が情報記録可能な装置である場合には、これをユニークに特定する情報を電子機器が書き加えるようにしてもよい。例えば、情報を記録可能な外部装置に対してフォーマット情報としてボリュームシリアル番号を記録されるようにすればよい。

【００３６】

これら装置をユニークに又はそれに準じて特定する情報を「装置特定情報」と定義すると、本発明における装置特定情報とは、機能に対して設定されている制限を解除するための暗証キーとして利用される情報と位置づけられる。

【００３７】

すなわち、特定の外部装置を示す装置特定情報を不揮発メモリなどに暗証キーとして予め記憶させておき、インタフェースを介して接続された外部装置から取得した装置特定情報が暗証キーと一致する場合に、機能に設定されている制限を解除する。

【００３８】

なお、図２に示すように、装置特定情報はその情報の種類によって外部装置をどの程度特定できるか（特定度）が異なる。例えば、装置特定情報がシリアル番号である場合は外部装置を１台に特定できるが、ロット番号である場合には、そのロットにおいて製造された装置のいずれかであるとしか特定できないことになる。

本発明は電子機器に上記動作を実行させることによって、電子機器の盗難や、情報の盗用の防止を図るものである。なお、図１中に破線で示すように、電子機器が上記動作の少なくとも一部を実質的なコンピュータによるソフトウエア処理で行うことも可能である。この場合は、従来と同様の構成のハードウエアを適用して本発明を実施することが可能となる。

以下、本発明の好適な実施の形態について説明する。

【００３９】

〔第１の実施形態〕

本発明を好適に実施した第１の実施形態について説明する。

図２に、本発明の第１の実施形態による不正使用防止プログラムを適用した電子機器１００を示す。電子機器１００は、制御部１０１、動作制限部１０２、外部装置情報取得部１０３、比較部１０４、ＮＶＲＡＭ１０５、Ｉ／Ｆ１０６及び書込制御部１０７を有する。制御部１０１は、電子機器１００が本来備える機能（例えば、演算機能、通信機能など）を実行させるための機能部である。動作制限部１０２は、電子機器１００が本来備える機能の少なくとも一部を制御部１０１が実行できないように制限（機能制限）を設定したり、その制限を解除したりする。外部装置情報取得部１０３は、Ｉ／Ｆ１０６を介して接続された外部装置から装置特定情報（ＣＩＳタプル、シリアル番号など）を取得する機能部である。比較部１０４は、ＮＶＲＡＭ１０５に暗証キーとして登録されている装置特定情報と、Ｉ／Ｆ１０６を介して接続されている外部装置から取得した装置特定情報とを比較し、一致するか否かを判断する。ＮＶＲＡＭ１０５は、電子機器の機能に設定されている制限を解除するか否かを判断する基準となる暗証キーが格納される。Ｉ／Ｆ１０６は、外部装置を接続するためのインタフェースであり、ＰＣカードスロット、ＵＳＢコネクタ、シリアルポート、パラレルポートなどの公知のものを適用可能である。書込制御部部１０７は、外部装置情報取得部１０３が外部装置から取得した装置特定情報を基に、Ｉ／Ｆ１０６を介して接続されている外部装置の種類や装置特定情報が外部装置をどの程度特定する情報であるか（ユニーク、製品レベル、製造元レベルなど）を判断する。また、接続された外部装置が情報記録可能な装置であり、かつ、その装置特定情報が装置をユニークに示す情報ではない場合は、装置をユニークに示す情報を生成し、これを外部装置に記憶させる。

【００４０】

図４に、Ｉ／Ｆ１０６を介して電子機器１００に接続された外部装置をユニークに特定する情報を暗証キーとしてＮＶＲＡＭ１０５に登録する場合の動作の流

れを示す。

Ｉ／Ｆ１０６に外部装置が接続されると、外部装置情報取得部１０３は、接続された外部装置から装置特定情報を取得する（ステップＳ１０１）。なお、Ｉ／Ｆ１０６に外部装置が接続されていない場合、外部装置情報取得部１０３は、外部装置が接続されていないことを示す情報を装置特定情報として取得する。書込制御部１０７は、外部装置情報取得部１０３が外部装置から取得した装置特定情報を基に、接続された外部装置が情報記録可能な装置であるか否かを判断する（ステップＳ１０２）。

【００４１】

接続された外部装置が情報記録可能な装置である場合（ステップＳ１０２／Ｙｅｓ）、書込制御部部１０７は、外部装置情報取得部１０３が取得した装置特定情報が装置をユニークに示す情報であるか否かを判断する（ステップＳ１０３）。装置特定情報が装置をユニークに示す情報ではない場合（ステップＳ１０３／Ｎｏ）、書込制御部部１０７は、装置をユニークに示す情報を生成し（ステップＳ１０４）、これを外部装置に記録させる（ステップＳ１０５）。これにより、これ以降に外部装置情報取得部１０３がこの外部装置から装置特定情報を取得する場合は、ステップＳ１０５で書き込んだ情報が装置特定情報として取得されることになる。その後、書込制御部部１０７は、外部装置に記録させた情報と同じ情報をＮＶＲＡＭ１０５に出力し、機能制限を解除するための暗証キーとして登録する（ステップＳ１０６）。

【００４２】

一方、Ｉ／Ｆ１０６を介して接続された外部装置が情報記録可能な装置でない場合や（ステップＳ１０２／Ｎｏ）、外部装置から取得した装置特定情報が装置をユニークに示す情報である場合（ステップＳ１０３／Ｙｅｓ）、書き込み制御部１０７は、外部装置情報取得部１０３が外部装置から取得した装置特定情報をそのままＮＶＲＡＭ１０５へ出力し、機能制限を解除するための暗証キーとして登録する（ステップＳ１０６）。

【００４３】

図５に、電子機器の機能に設定されている制限をＩ／Ｆ１０６を介して接続し

た外部装置を用いて解除する際の動作の流れを示す。

Ｉ／Ｆ１０６に外部装置が接続されると、外部装置情報取得部１０３は、接続された外部装置から装置特定情報を取得する（ステップＳ２０１）。比較部１０４は、現在Ｉ／Ｆ１０６に接続されている外部装置の装置特定情報を外部装置情報取得部１０３から取得するとともに、ＮＶＲＡＭ１０５に暗証キーとして登録されている装置特定情報を読み出す（ステップＳ２０２）。比較部１０４は、これらの情報を比較し、一致するか否かを判断する（ステップＳ２０３）。

【００４４】

比較結果が一致する場合（ステップＳ２０３／Ｙｅｓ）、比較部１０４は動作制限部１０２に指示を送り、動作制限部１０２が制御部１０１に対して設定している制限を解除し、制限されていた機能を使用できるようにする（ステップＳ２０４）。

一方、比較結果が一致しない場合は（ステップＳ２０３／Ｎｏ）、制御部１０１に対して設定されている制限を解除しない。

【００４５】

このように、機能制限を解除する動作を一度だけ実行する場合は、機能制限を解除する際に暗証キーとなる外部装置が接続されていればよく、機能制限を解除した後に暗証キーとなる外部装置を取り外しても電子機器１００は使用可能となる。このため、使用頻度の低い外部装置を暗証キーとしてＮＶＲＡＭ１０５に登録した場合には、機能制限を解除した後にその外部装置を取り外し、Ｉ／Ｆ１０６に別の外部装置を接続して使用することが可能となる。

【００４６】

また、機能制限を解除する動作を定期的に行うようにしてもよい。図６に、この場合の電子機器１００の動作の流れを示す。

ステップＳ２０１’～Ｓ２０４’の動作は、図５のステップＳ２０１～Ｓ２０４の動作と同様である。

ステップＳ２０３’の処理終了後所定の時間が経過すると（ステップＳ２０５’／Ｙｅｓ）、動作制限部１０２は、ステップＳ２０４’において解除した制限を再び制御部１０１に対して設定し、機能制限に係る機能を使用できない状態に

する（ステップＳ２０６）。

その後、ステップＳ２０１’に戻り、比較部１０４は、現在Ｉ／Ｆ１０６を介して接続されている外部装置から装置特定情報取得部１０３が取得した装置特定情報と、ＮＶＲＡＭ１０５に暗証キーとして登録されている情報とを比較して、機能制限を解除するか否かを決定する（ステップＳ２０１’～Ｓ２０３’）。

【００４７】

機能制限を解除する動作を定期的に行う場合は、一度機能制限を解除しても、所定時間経過後に暗証キーとしてＮＶＲＡＭ１０５に登録されている外部装置がＩ／Ｆ１０６を介して接続されているか否かを比較部１０４が再度判断するため、セキュリティ性を高めることが可能となる。

例えば、機能制限が解除された状態の電子機器１００を盗んだとしても、暗証キーとしてＮＶＲＡＭ１０５に登録された外部装置を所持していなければ、所定時間経過後に電子機器１００を使用できなくなるため、電子機器１００の盗難を抑止できる。

【００４８】

また、機能制限を再設定するまでの時間を短くすれば、暗証キーとしてＮＶＲＡＭ１０５に登録されている外部装置がＩ／Ｆ１０６を介して接続されていない限り電子機器１００を使用不能にできる。

例えば、Ｉ／Ｆ１０６を介して接続された外部装置から取得した装置特定情報をＮＶＲＡＭ１０５に暗証キーとして登録された情報と比較してから、機能制限を再設定するまでの間隔を１／１００秒とすれば、実質的には、暗証キーとして登録された外部装置が接続されていない状態で電子機器１００を使用することは不可能となる。

【００４９】

このように、電子機器１００は、機能制限を解除する動作を一度だけ行っても良いし、繰り返し行ってもよい。

換言すると、電子機器１００には、暗証キーとして登録された外部装置を利用開始時（機能制限解除時）のみ接続し、その後は接続を継続する必要のない利用形態と、利用期間中継続して接続しておく必要がある利用形態とがある。電子機

器１００をどちらの利用形態で利用するかは、電子機器１００が適用されるシステムの性格に応じて選択又は切り替えることが可能である。

【００５０】

本実施形態では、接続された外部装置から装置特定情報を取得する機能を備えた電子機器に対して、電子機器としての機能の少なくとも一部を実行できないように制限を施しておくとともに、特定の外部装置が接続されていること（すなわち、接続された外部装置から特定の装置特定情報を取得した場合）を制限を解除する条件として予め登録しておく。これにより、機能の制限を解除する条件として予め登録されている外部装置が接続された場合のみ、又は、接続されている場合のみ制限が施されている機能を利用することが可能となる。

【００５１】

〔第２の実施形態〕

本発明を好適に実施した第２の実施形態について説明する。

図７に、本実施形態による不正使用防止プログラムを適用した電子機器２００を示す。電子機器２００は、Ｉ／Ｆ１０６を複数（１０６ａ、１０６ｂ）備える他は、第１の実施形態の電子機器１００と同様である。

【００５２】

本実施形態においては、装置特定情報が単独で、又は、二つの装置特定情報を組としたものが機能制限を解除するための暗証キーとして用いられる。

【００５３】

図８に、ＮＶＲＡＭ１０５に暗号キーとして二つの装置特定情報からなる組を登録する場合の動作の流れを示す。

Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれに外部装置が接続されると、電子機器２００は、第１の実施形態のステップＳ３０１～Ｓ３０５と同様の処理を、Ｉ／Ｆ１０６ａや１０６ｂを介して接続された外部装置のそれぞれについて別個に行う（ステップＳ３０１ａ～Ｓ３０５ａ、ステップＳ３０１ｂ～Ｓ３０５ｂ）。

その後、書込制御部１０７は、Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれを介して接続されている外部装置について、装置特定情報、又は、外部装置に記録させた情報と同じ情報を、暗証キーとしてＮＶＲＡＭ１０５に登録する（ステップＳ

３０６）。

【００５４】

図９に、ＮＶＲＡＭ１０５に暗号キーとして二つの装置特定情報からなる組を登録した場合に、Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれを介して接続した外部装置を用いて電子機器の機能に設定されている制限を解除する動作の流れを示す。

【００５５】

Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれに外部装置が接続されると、外部装置情報取得部１０３は、それぞれの外部装置から装置特定情報を取得する（ステップＳ４０１ａ、Ｓ４０１ｂ）。なお、Ｉ／Ｆ１０６ａや１０６ｂに外部装置が接続されていない場合、外部装置情報取得部１０３は、外部装置が接続されていないことを示す情報を装置特定情報として取得する。比較部１０４は、現在Ｉ／Ｆ１０６ａ、１０６ｂにそれぞれ接続されている外部装置の装置特定情報を外部装置情報取得部１０３から取得するとともに、ＮＶＲＡＭ１０５に暗証キーとして登録されている装置特定情報の組を読み出す（ステップＳ４０２）。さらに比較部１０４は、現在Ｉ／Ｆ１０６ａ及び１０６ｂを介して接続されている外部装置の組合せ（すなわち、装置特定情報の組合せ）が、暗証キーとして登録されている装置特定情報の組合せと一致するか否かを判断する（ステップＳ４０３）。

【００５６】

比較結果が一致する場合（ステップＳ４０３／Ｙｅｓ）、比較部１０４は動作制限部１０２に指示を送り、動作制限部１０２が制御部１０１に対して設定している制限を解除し、制限されていた機能を使用できるようにする（ステップＳ４０４）。

一方、比較結果が一致しない場合（ステップＳ４０３／Ｎｏ）、動作制限部１０２は、特定の機能の制限を引き続いて行う。

【００５７】

図１０に、ＮＶＲＡＭ１０５に暗号キーとして一つの装置特定情報を単独で登録した場合に、Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれを介して接続した外部装置を用いて、制限されている電子機器の機能を復帰させる動作の流れを示す。

【００５８】

Ｉ／Ｆ１０６ａ及び１０６ｂの少なくともいずれかに外部装置が接続されると、外部装置情報取得部１０３は、それぞれの外部装置から装置特定情報を取得する（ステップＳ５０１ａ、Ｓ５０１ｂ）。なお、Ｉ／Ｆ１０６ａや１０６ｂに外部装置が接続されていない場合、外部装置情報取得部１０３は、外部装置が接続されていない旨を示す情報を装置特定情報として取得する。比較部１０４は、現在Ｉ／Ｆ１０６ａに接続されている外部装置の装置特定情報を外部装置情報取得部１０３から取得するとともに、ＮＶＲＡＭ１０５に暗証キーとして登録されている装置特定情報を読み出す（ステップＳ５０２）。さらに比較部１０４は、現在Ｉ／Ｆ１０６ａ又は１０６ｂに接続されているいずれかの外部装置の装置特定情報と、機能制限を解除するための暗証キーとして登録されている装置特定情報とを比較し、一致するか否かを判断する（ステップＳ５０３）。

【００５９】

比較結果が一致する場合（ステップＳ５０３／Ｙｅｓ）、比較部１０４は動作制限部に指示を送り、動作制限部１０２が制御部１０１に対して設定している制限を解除し、制限されていた機能を使用できるようにする。

一方、比較結果が一致しない場合、（ステップＳ５０３／Ｎｏ）、動作制限部１０２は、特定の機能の制限を引き続いて行う。

【００６０】

なお、ここでは電子機器がＩ／Ｆ１０６を二つ（１０６ａ及び１０６ｂ）備える場合を例に説明を行ったが、Ｉ／Ｆ１０６を三つ以上備えていてもよい。例えば、Ｉ／Ｆ１０６を三つ備える場合は、ＮＶＲＡＭ１０５には、三つの装置特定情報の組合せ、二つの装置特定情報の組合せ、及び、一つの装置特定情報を単独で暗証キーとして登録することが可能となる。

すなわち、Ｉ／Ｆ１０６をｎ個（ｎは３以上の自然数）備える場合は、ＮＶＲＡＭ１０５にはｎ個～２個の装置特定情報の組合せ、又は装置特定情報を単独で暗証キーとして登録することが可能となる。

また、本実施形態においても機能制限を解除する動作を繰り返し実行するようにしてもよい。この場合は第１の実施形態と同様に、装置特定情報と暗証キーと

の比較を行った後所定の時間が経過した時点で機能制限を再設定し、再び装置特定情報と暗証キーとの比較を行う処理となるため説明は省略する。

【００６１】

このように、本実施形態では、接続された外部装置から装置特定情報を取得する機能を備えた電子機器に対して、電子機器としての機能の少なくとも一部を実行できないように制限を施しておくとともに、特定の外部装置が接続されていること（すなわち、接続された外部装置から特定の装置特定情報を取得した場合）を制限を解除する条件として予め登録しておく。これにより、機能の制限を解除する条件として予め登録されている外部装置が接続された場合のみ、又は、接続されている場合のみ制限が施されている機能を利用することが可能となる。

また、電子機器の機能の制限を解除する条件として、複数の外部装置の組合せを予め登録しておけば、この組合せに係る外部装置が全て接続されている場合のみ、制限が施されている機能を利用することなどが可能となる。

【００６２】

〔第３の実施形態〕

本発明を好適に実施した第３の実施形態について説明する。

図１１に、本実施形態による不正使用防止プログラムを適用した電子機器３００を示す。電子機器３００は、Ｉ／Ｆ１０６及び外部装置情報取得部１０３を二つずつ備える他は、第２の実施形態による電子機器２００と同様である。

外部装置情報取得部１０３ａは、Ｉ／Ｆ１０６ａを介して接続された外部装置から装置特定情報を取得する。また、外部装置情報取得部１０３ｂは、Ｉ／Ｆ１０６ｂを介して接続された外部装置から装置特定情報を取得する。外部装置情報取得部１０３ａ、１０３ｂが取得した装置特定情報は、第２の実施形態と同様に、暗証キーとしてＮＶＲＡＭ１０５に格納されたり、機能制限を解除するか否かを判断するために用いられる。

【００６３】

図１２に、ＮＶＲＡＭ１０５に暗号キーとして二つの装置特定情報からなる組を登録する場合の動作の流れを示す。

ステップＳ６０１ａ～Ｓ６０５ａ、及び、ステップＳ６０１ｂ～Ｓ６０５ｂの

動作は、第２の実施形態のステップＳ３０１～Ｓ３０５ａ、ステップＳ３０１ｂ～Ｓ３０５ｂとそれぞれ同様である。

ステップＳ６０６において、書込制御部１０７は、Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれを介して接続されている外部装置について、装置特定情報、又は、外部装置に記録させた情報と同じ情報を、暗証キーとしてＮＶＲＡＭ１０５に登録する。

【００６４】

本実施形態においては、Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれを介して接続されている外部装置からの装置特定情報は、各々が別個の伝送路を経て書込制御部１０７へ入力される。このため、書込制御部１０７においては、外部装置情報取得部１０３ａ及び１０３ｂが取得した装置特定情報はそれぞれ別個に扱われる。これにより、電子機器３００は、同一の外部装置であっても、Ｉ／Ｆ１０６ａを介して接続された場合と、Ｉ／Ｆ１０６ｂを介して接続された場合とを区別することができる。

図１３に、書込制御部１０７がＮＶＲＡＭ１０５に登録する暗証キーの一例を示す。同図に示すように、本実施形態においては、どの外部装置が接続されているかだけでなく、その外部装置がどのインタフェースを介して接続されているかをも含めた条件を機能制限を解除するための暗証キーとして登録することが可能となる。

【００６５】

図１４に、ＮＶＲＡＭ１０５に暗号キーとして二つの装置特定情報からなる組を登録した場合に、Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれを介して接続した外部装置を用いて電子機器の機能に設定されている制限を解除する動作の流れを示す。

【００６６】

Ｉ／Ｆ１０６ａ及び１０６ｂのそれぞれに外部装置が接続されると、外部装置情報取得部１０３ａ及び１０３ｂは、それぞれの外部装置から装置特定情報を取得する（ステップＳ７０１ａ、Ｓ７０１ｂ）。なお、Ｉ／Ｆ１０６ａや１０６ｂに外部装置が接続されていない場合、外部装置情報取得部１０３ａや１０３ｂは

、外部装置が接続されていないことを示す情報を装置特定情報として取得する。比較部１０４は、現在Ｉ／Ｆ１０６ａ、１０６ｂにそれぞれ接続されている外部装置の装置特定情報を外部装置情報取得部１０３ａ及び１０３ｂから取得するとともに、ＮＶＲＡＭ１０５に暗証キーとして登録されている装置特定情報の組を読み出す（ステップＳ７０２）。さらに比較部１０４は、現在Ｉ／Ｆ１０６ａ及び１０６ｂを介して接続されている外部装置の組合せ（すなわち、装置特定情報の組合せ）が、暗証キーとして登録されている装置特定情報の組合せと一致するか否かを判断する（ステップＳ７０３）。

【００６７】

比較結果が一致する場合（ステップＳ７０３／Ｙｅｓ）、比較部１０４は、現在接続されている各外部装置が、装置特定情報を暗証キーとして登録した時と同じインタフェースを介して接続されているか否かを判断する（ステップＳ７０４）。同じインタフェースを介して接続されている場合は（ステップＳ７０４／Ｙｅｓ）、比較部１０４は動作制限部１０２に指示を送り、動作制限部１０２が制御部１０１に対して設定している制限を解除し、制限されていた機能を使用できるようにする（ステップＳ７０５）。

【００６８】

現在Ｉ／Ｆ１０６ａ及び１０６ｂを介して接続されている外部装置から取得した装置特定情報の組合せが、暗証キーとしてＮＶＲＡＭ１０５に登録されている装置特定情報の組合せと一致しない場合（ステップＳ７０３／Ｎｏ）、又は、装置特定情報を暗証キーとして登録した時と異なるインタフェースを介して接続されている場合（ステップＳ７０４／Ｎｏ）、動作制限部１０２は、特定の機能の制限を引き続いて行う。

【００６９】

このように、本実施形態においては、電子機器は外部装置がどのインタフェースを介して接続されているかを区別できる。これにより、例えば、Ｉ／Ｆ１０６ａを介して接続された外部装置Ａから取得した装置特定情報と、Ｉ／Ｆ１０６ｂを介して接続された外部装置Ｂから取得した装置特定情報との組み合わせがＮＶＲＡＭ１０５に暗証キーとして登録されている場合は、Ｉ／Ｆ１０６ａを介して

外部装置Ｂを接続し、Ｉ／Ｆ１０６ｂを介して外部装置Ａを接続しても、機能の制限を解除することはできない。

すなわち、本実施形態では、電子機器の盗難を抑止したり、情報の盗用を防止したりする効果を第２の実施形態よりも高いレベルで得ることができる。

【００７０】

なお、第２の実施形態と同様に、ここでは電子機器がＩ／Ｆ１０６を二つ（１０６ａ及び１０６ｂ）備える場合を例に説明を行ったが、Ｉ／Ｆ１０６を三つ以上備えていてもよい。Ｉ／Ｆ１０６を三つ備える場合は、ＮＶＲＡＭ１０５には、三つの装置特定情報の組合せ、二つの装置特定情報の組合せ、及び、一つの装置特定情報を単独で暗証キーとして登録することが可能となる。

すなわち、Ｉ／Ｆ１０６をｎ個（ｎは３以上の自然数）備える場合は、ＮＶＲＡＭ１０５にはｎ個～２個の装置特定情報の組合せ、又は装置特定情報を単独で暗証キーとして登録することが可能となる。

また、本実施形態においても機能制限を解除する動作を繰り返し実行するようにしてもよい。この場合は第１の実施形態と同様に、装置特定情報と暗証キーとの比較を行った後所定の時間が経過した時点で機能制限を再設定し、再び装置特定情報と暗証キーとを比較する処理となるため、説明は省略する。

【００７１】

本実施形態において、電子機器３００のＮＶＲＡＭ１０５には、外部装置から取得した装置特定情報に加えて、外部装置がどのインタフェースを介して接続されているかを暗証キーとして登録できる。このため、機能制限を解除するためのキーとなる外部装置が電子機器３００と共に盗まれたとしても、暗証キーを登録した時と同一のインタフェースを介して電子機器３００に接続されなければ、電子機器３００に設定されている機能制限は解除されない。これにより、機能制限を解除する条件を知らない者が電子機器３００を不正に使用したり、情報を盗用することは困難となるため、電子機器３００が盗まれたり、情報が盗用されることを防止できる。

【００７２】

〔第４の実施形態〕

本発明を好適に実施した第４の実施形態について説明する。本実施形態においては、電子機器に機能制限が多段階に分けて設定されており、接続された外部装置から取得した装置特定情報に応じて制限を解除する程度を変更する。

【００７３】

本実施形態においては、第１の実施形態と同様の電子機器を適用できる。電子機器に対して設定される機能制限は、ＮＶＲＡＭ１０５に機能制限テーブルとして登録される。図１５に、この一例を示す。

【００７４】

「利用可能機能」は、電子機器１００の機能のうちどの機能が利用可能とするかを示しており、“Ｎｏｔｈｉｎｇ”は全ての機能が利用不可とすることを、“Ｒｅａｄ”は、データの読み出しを可能とすることを、“Ｗｒｉｔｅ”はデータの書込を可能とすることを、“Ａｌｌ”はシステムの設定を含めて全ての機能を利用可能とすることを示している。

「暗証キー」は、機能制限を解除する条件を示しており、“Ａ”、“Ｂ”、“Ｃ”は、Ｉ／Ｆ１０６を介して“外部装置Ａ”、“外部装置Ｂ”、“外部装置Ｃ”が接続されることをそれぞれ示している。なお、“Ｄｅｆａｕｌｔ”は、初期状態（常態）を示す。

【００７５】

図１６に、上記条件がＮＶＲＡＭ１０５に機能制限テーブルとして登録されている電子機器において、電子機器に設定されている機能制限をＩ／Ｆ１０６に接続された外部装置を用いて解除する場合の動作の流れを示す。

Ｉ／Ｆ１０６を介して外部装置が接続されると、外部装置情報取得部１０３は、接続された外部装置から装置特定情報を取得する（ステップＳ８０１）。比較部１０４は、外部装置情報取得部１０３から現在Ｉ／Ｆ１０６を介して接続されている外部装置の装置特定情報を取得するとともに、ＮＶＲＡＭ１０５から機能制限テーブルを読み出す。比較部１０４は、機能制限テーブルに暗証キーとして登録されている装置特定情報の中に、外部装置情報取得部１０３から取得した装置特定情報があるか否かを判定する（ステップＳ８０２）。

【００７６】

外部装置情報取得部１０３から取得した装置特定情報が“Ａ”であった場合、すなわち、Ｉ／Ｆ１０６を介して外部装置Ａが接続されている場合（ステップＳ８０２／Ａ）、動作制限部１０２は、制御部１０１に対して設定している制限を全て解除して、電子機器１００の機能を全て使用可能とする（ステップＳ８０３）。

【００７７】

外部装置情報取得部１０３から取得した装置特定情報が“Ｂ”であった場合、すなわち、Ｉ／Ｆ１０６を介して外部装置Ｂが接続されている場合（ステップＳ８０２／Ｂ）、動作制限部１０２は、制御部１０１に対して設定している制限のうち、情報の書き込み・読み出しに関する機能の制限のみを解除する（ステップＳ８０４）。

【００７８】

外部装置情報取得部１０３から取得した装置特定情報が“Ｃ”であった場合、すなわち、Ｉ／Ｆ１０６を介して外部装置Ｃが接続されている場合（ステップＳ８０２／Ｃ）、動作制限部１０２は、制御部１０１に対して設定している制限のうち、情報の読み出しに関する機能の制限のみを解除する（ステップＳ８０５）。

【００７９】

外部装置情報取得部１０３から取得した装置特定情報が“Ａ”、“Ｂ”及び“Ｃ”のいずれでもない場合、又は、外部装置情報取得部１０３から取得した装置特定情報が、外部装置が接続されていないことを示している場合（ステップＳ８０２／その他）、動作制限部１０２は、制御部１０１に対して設定している制限をいずれも解除せず、全ての機能を使用不可とする状態を継続させる（ステップＳ８０６）。

【００８０】

本実施形態の電子機器１００の動作について具体的な例を挙げて説明する。ここでは、電子機器１００を用いたシステムを管理する「システム管理者Ａ」、常時システムを利用する「利用者Ｂ」、一時的にシステムを利用する「利用者Ｃ」及び「利用者Ｄ」、システムの使用する権限がない「部外者Ｅ」が存在するもの

とする。

【００８１】

システム管理者Ａは、ＮＶＲＡＭ１０５に外部装置Ａ、Ｂ及びＣを暗証キーとして上記同様の機能制限を設定しておく。登録後、外部装置Ａは自身が所持し、外部装置Ｂは利用者Ｂに手渡す。また、外部装置Ｃは一時利用者用に貸し出す準備をしておく。

【００８２】

常態においてはシステムの全ての機能に制限が設定されているため、システムを利用しようとする各人は、手持ちの外部装置を用いて、機能制限を解除しなければならない。

例えば、利用者Ｂがシステムを使用する場合は、自身に割り当てられた外部装置Ｂを用いて機能制限を解除する。また、利用者Ｃがシステムを使用したい場合は、システム管理者Ａに許可を得て外部装置Ｃを借用し、機能制限を解除した上で使用システムを使用し、使用後に外部装置Ｂを返却する。利用者Ｄがシステムを使用する場合は、利用者Ｃと同様である。

部外者Ｅが不正に（管理者Ａの許可を得ずに）システムを使用しようとした場合は、機能制限を解除できないため、システムを使用することはできない。

【００８３】

なお、ここでは、電子機器１００がインタフェースとしてＩ／Ｆ１０６を一つだけ備える場合を例に説明を行ったが、第２の実施形態や第３の実施形態と同様に、電子機器１００はＩ／Ｆ１０６を複数備えていても良い。

【００８４】

このように、本実施形態によれば、電子機器の盗難や情報の盗用を抑止できるとともに、多段階に設定された機能制限を電子機器に接続された外部装置の種類に応じて解除することで、多段階のセキュリティーを電子機器に設定できる。

本実施形態においても、機能制限を解除する動作を繰り返し実行するようにしてもよい。この場合は第１の実施形態と同様に、外部装置から取得した装置特定情報と暗証キーとを比較した後所定の時間が経過した時点で機能制限を再設定し、再び外部装置から取得した装置特定情報と暗証キーとを比較する処理であるた

め説明は省略する。

【００８５】

なお、上記各実施形態は、本発明の好適な実施の一例であり、本発明はこれに限定されるものではない。

例えば、上記実施形態では外部装置情報取得部１０３が情報記録可能な外部装置から取得した装置特定情報が装置をユニークに示すものでない場合に、この装置に対して装置をユニークに示す情報を付与しているが、本発明はこれに限定されるものではない。

【００８６】

また、上記各実施形態においては、暗証キーをＮＶＲＡＭ１０５に格納しているが、情報を不揮発に保存できればどのような記憶装置を用いても構わない。例えば、情報量が多い場合には、ハードディスクドライブのような容量の大きい記憶装置を用いてもよい。

【００８７】

さらに、上記各実施形態における暗証キーや制限テーブルのデータ構造は、あくまでも一例であり、これに限定されるものではない。

このように、本発明は様々な変形が可能である。

【００８８】

【発明の効果】

以上の説明によって明らかなように、本発明によれば、不特定多数人が利用可能な環境に設置された電子機器の盗難を防止するとともに、電子機器に記憶された情報が盗用されることを防止する電子機器及びその不正使用防止方法並びにその不正使用防止プログラムを提供できる。

【図面の簡単な説明】

【図１】

本発明の概要を説明するための図である。

【図２】

装置特定情報の種類の及びその特定度の関係の一例を示す図である。

【図３】

本発明を好適に実施した第１の実施形態に係る電子機器の構成を示す図である。

【図４】

第１の実施形態に係る電子機器が暗証キーを登録する場合の動作の流れの一例を示す図である。

【図５】

第１の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

【図６】

第１の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの別の一例を示す図である。

【図７】

本発明を好適に実施した第２の実施形態に係る電子機器の構成を示す図である。

【図８】

第２の実施形態に係る電子機器が暗証キーを登録する場合の動作の流れの一例を示す図である。

【図９】

第２の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

【図１０】

第２の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

【図１１】

本発明を好適に実施した第３の実施形態に係る電子機器の構成を示す図である。

【図１２】

第３の実施形態に係る電子機器が暗証キーを登録する場合の動作の流れを示す図である。

【図１３】

第３の実施形態における暗証キーの一例を示す図である。

【図１４】

第３の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

【図１５】

機能制限テーブルの一例を示す図である。

【図１６】

本発明を好適に実施した第４の実施形態に係る電子機器が機能制限解除する場合の動作の流れの一例を示す図である。

【符号の説明】

１００、２００、３００　電子機器

１０１　制御部

１０２　動作制限部

１０３、１０３ａ、１０３ｂ　外部装置情報取得部

１０４　比較部

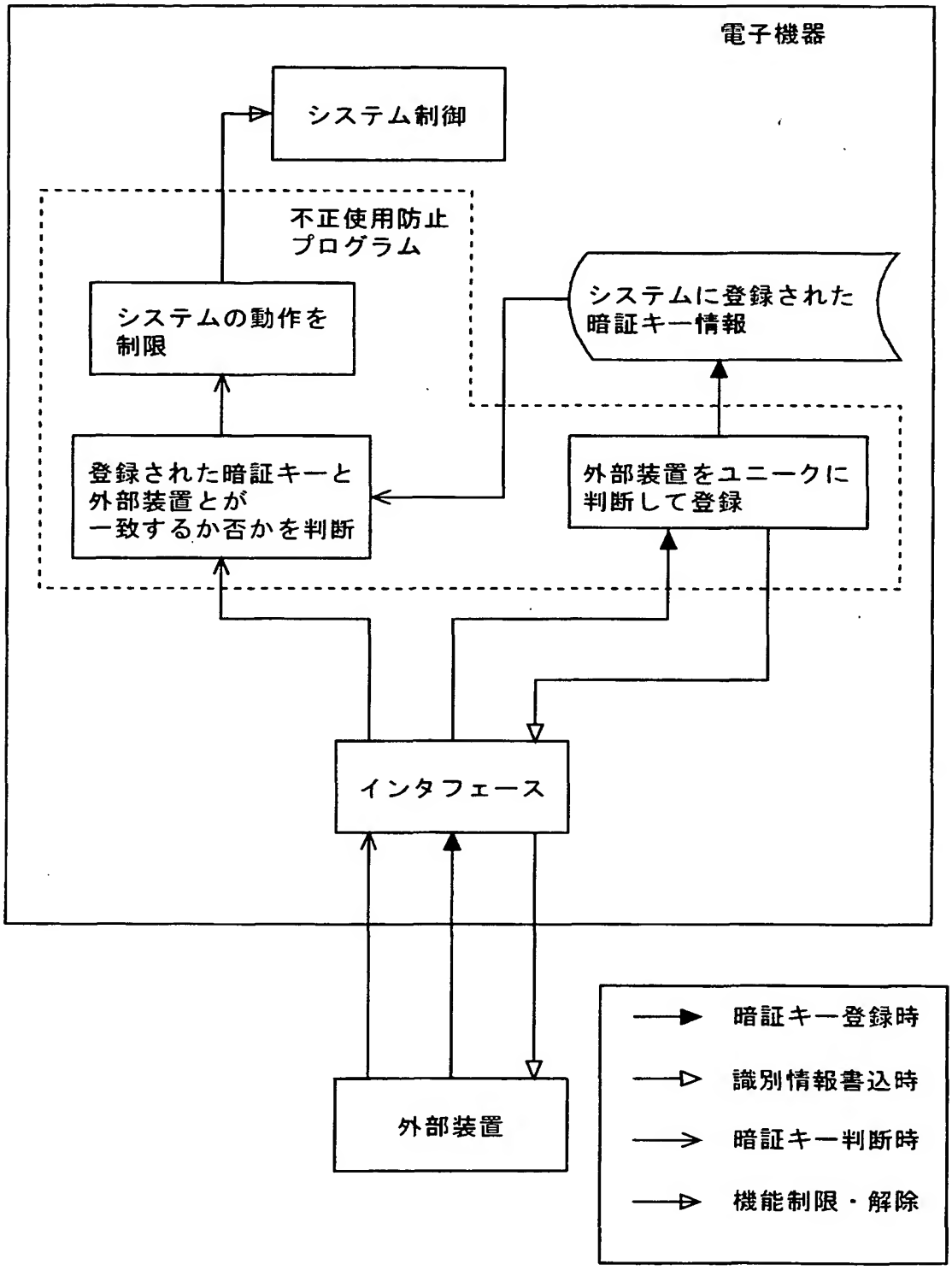
１０５　ＮＶＲＡＭ

１０６、１０６ａ、１０６ｂ　インタフェース（Ｉ／Ｆ）

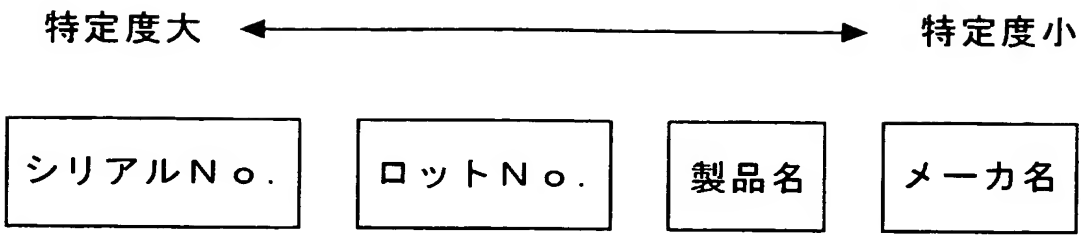
１０７　書込制御部

【書類名】　　図面

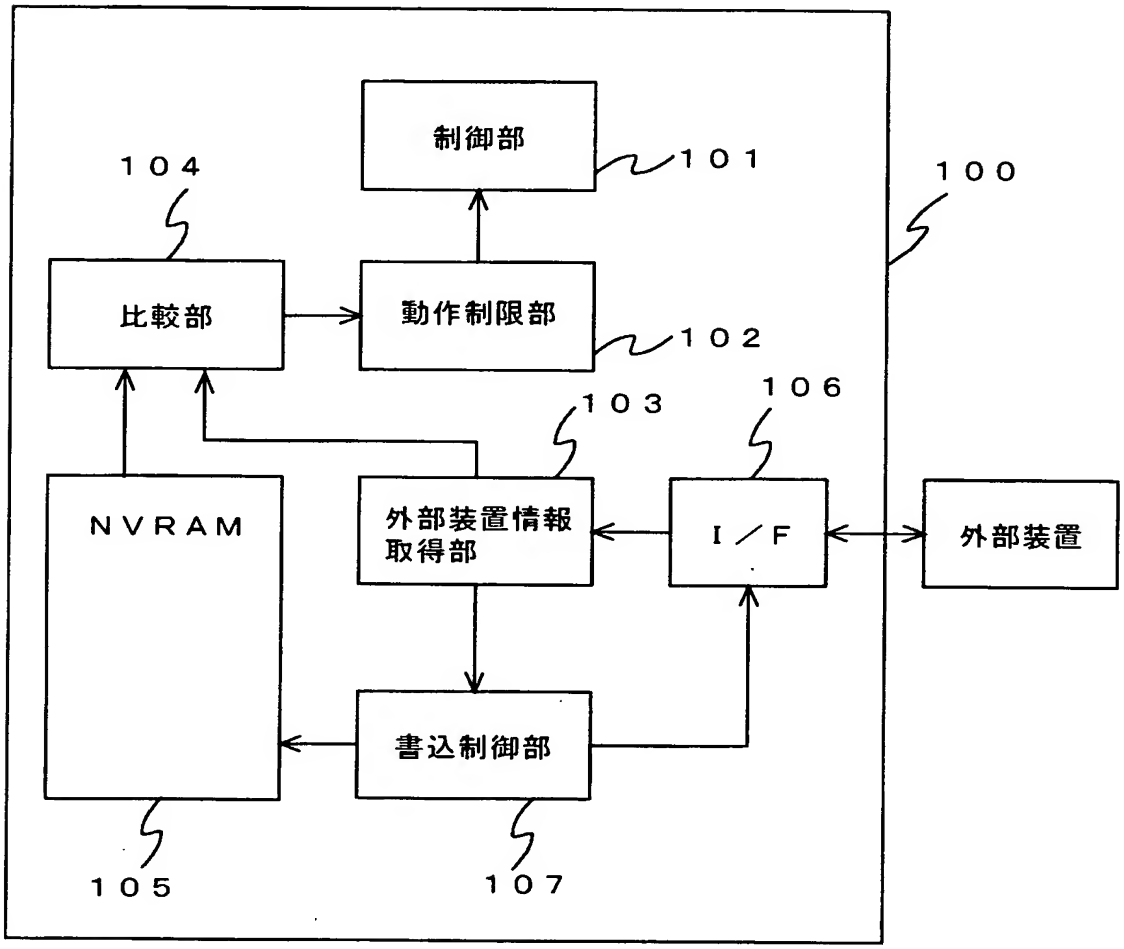
【図１】


電子機器
システム制御
不正使用防止
プログラム
システムの動作を
制限
システムに登録された
暗証キー情報
登録された暗証キーと
外部装置とが
一致するか否かを判断
外部装置をユニークに
判断して登録
インタフェース
外部装置
暗証キー登録時
識別情報書込時
暗証キー判断時
機能制限・解除

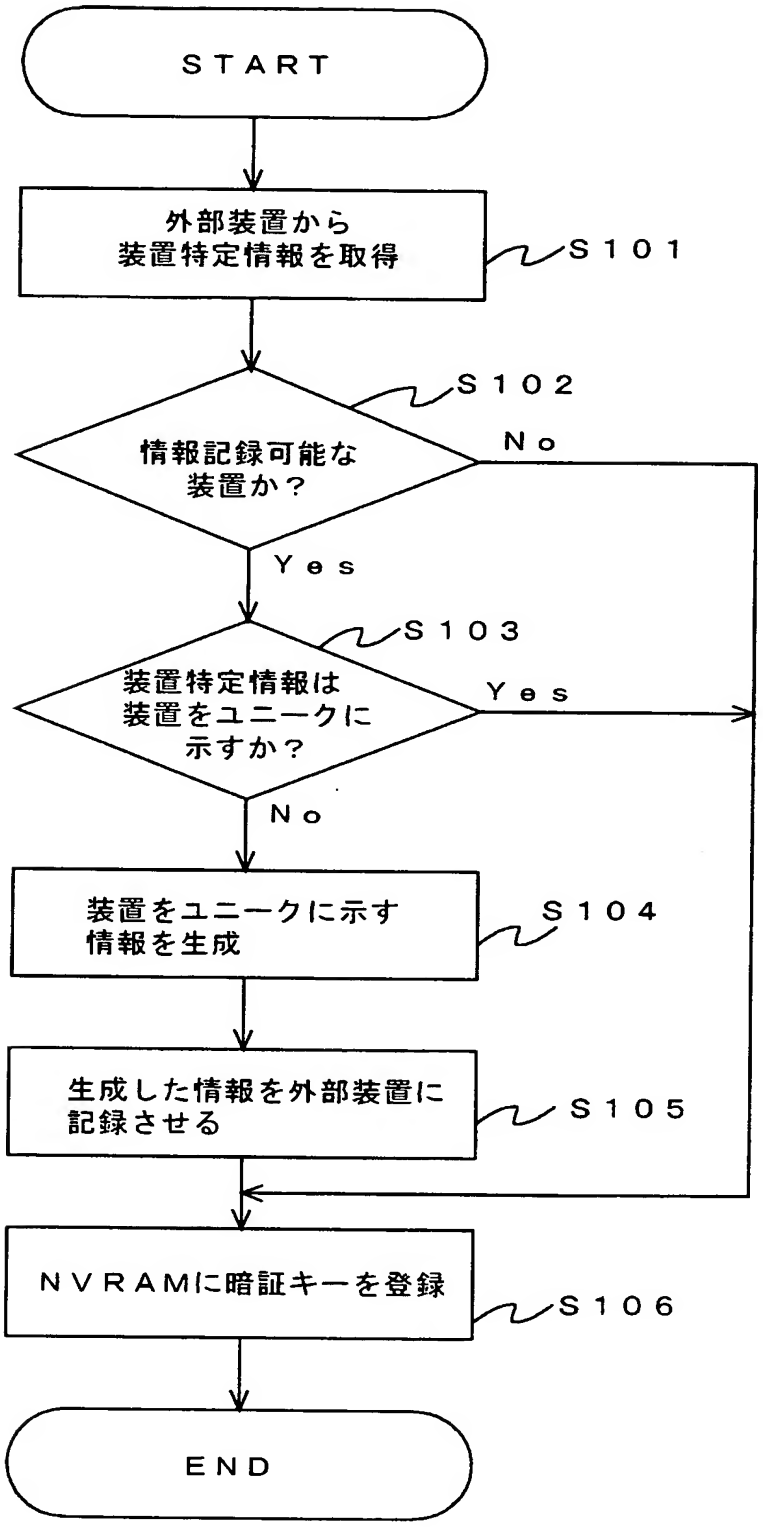
【図２】


特定度大
特定度小
シリアルＮｏ．
ロットＮｏ．
製品名
メーカ名

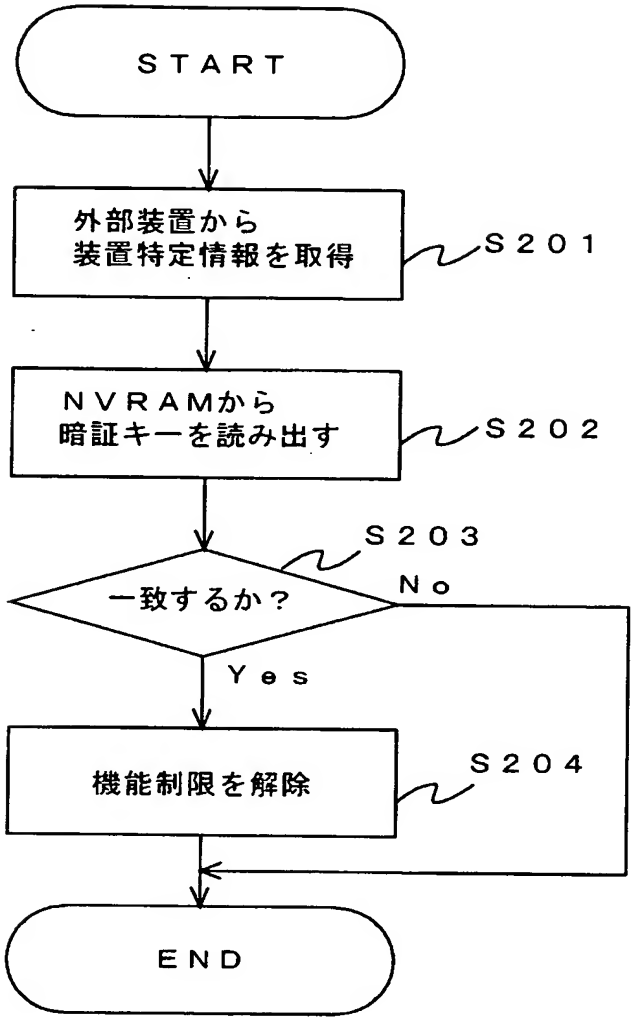
【図３】


制御部
１０１
１００
１０４
比較部
動作制限部
１０２
１０３
１０６
NVRAM
外部装置情報
取得部
Ｉ／Ｆ
外部装置
書込制御部
１０５
１０７

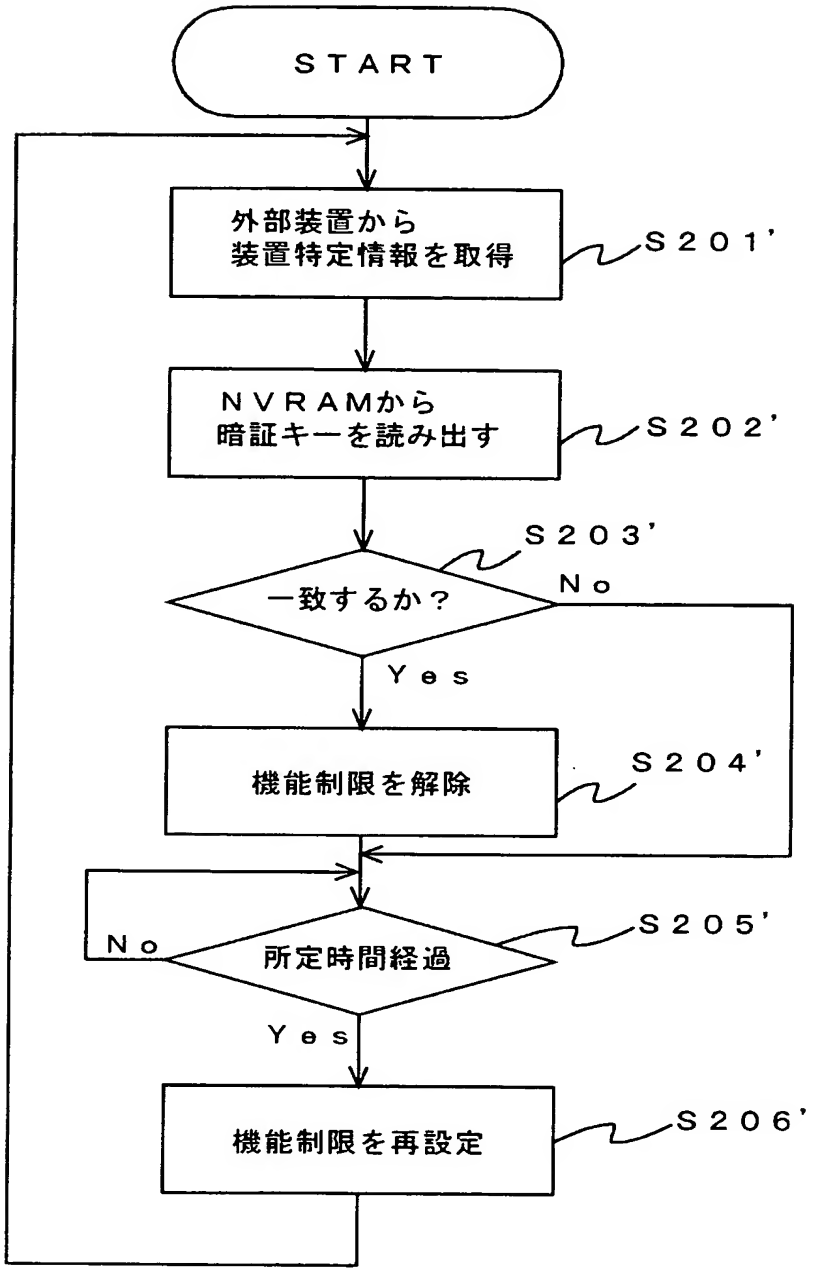
【図４】


START
外部装置から
装置特定情報を取得
S１０１
S１０２
情報記録可能な
装置か？
No
Yes
S１０３
装置特定情報は
装置をユニークに
示すか？
Yes
No
装置をユニークに示す
情報を生成
S１０４
生成した情報を外部装置に
記録させる
S１０５
NVRAMに暗証キーを登録
S１０６
END

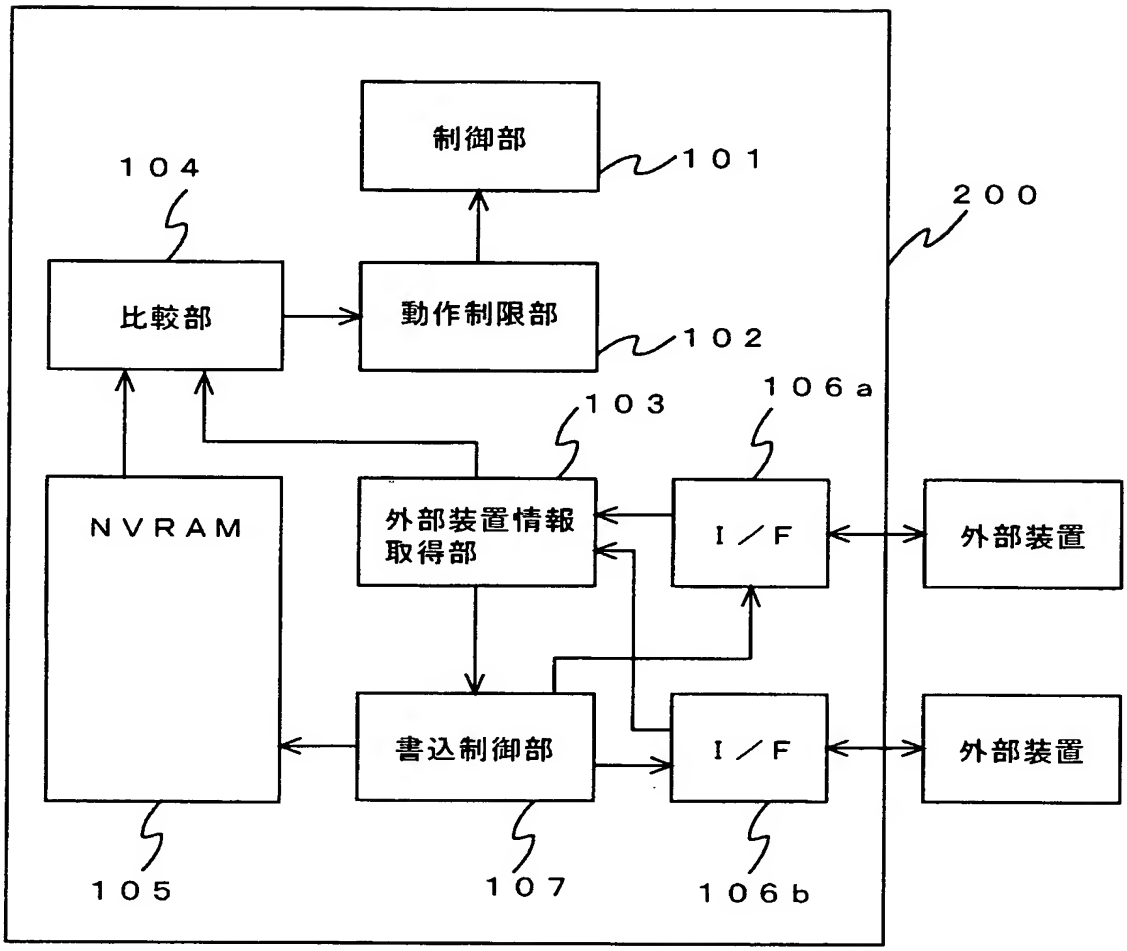
【図５】


START
外部装置から
装置特定情報を取得
S２０１
NVRAMから
暗証キーを読み出す
S２０２
S２０３
一致するか？
No
Yes
機能制限を解除
S２０４
END

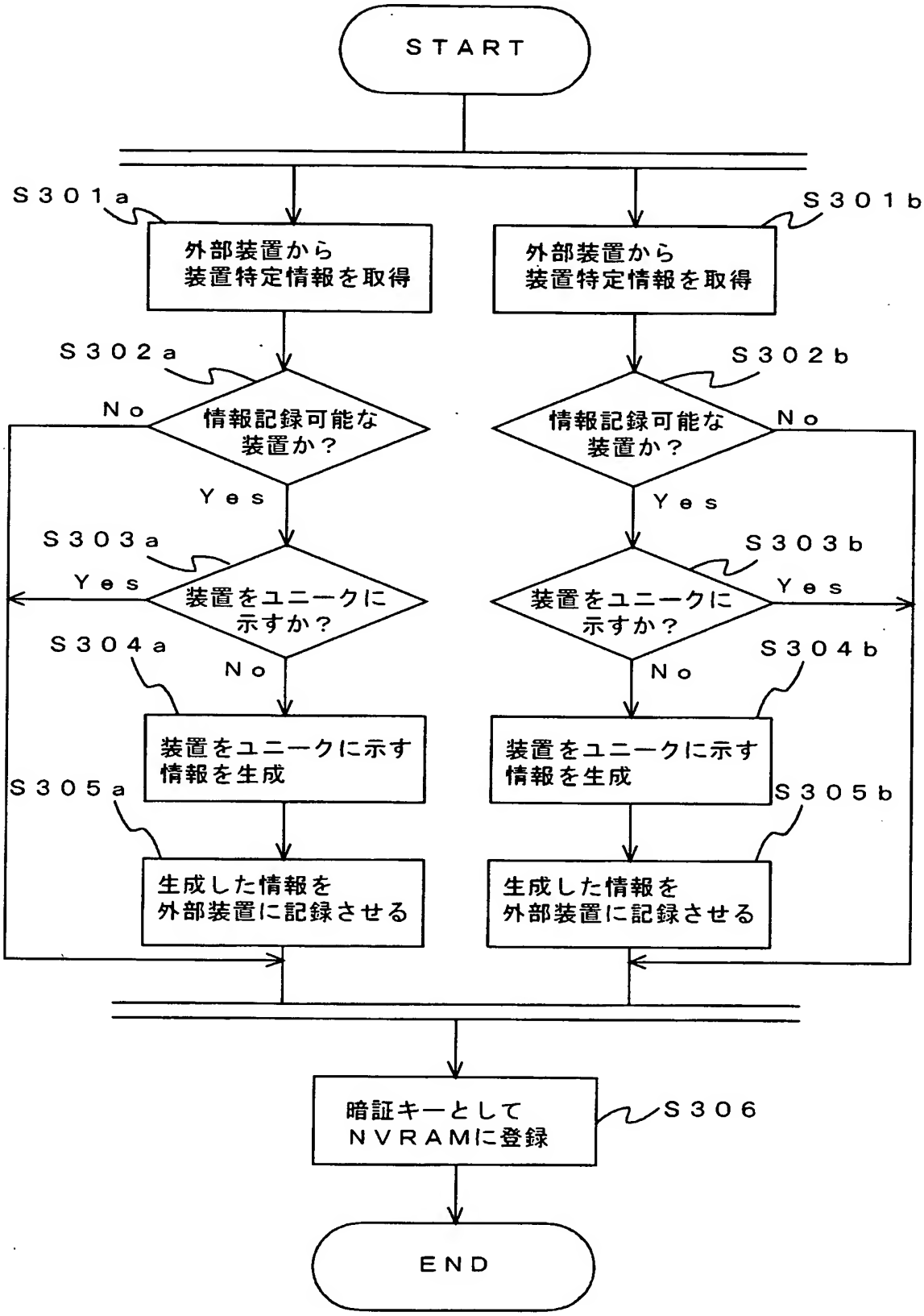
【図６】


START
外部装置から
装置特定情報を取得
S２０１'
ＮＶＲＡＭから
暗証キーを読み出す
S２０２'
S２０３'
一致するか？
No
Ｙｅｓ
機能制限を解除
S２０４'
No
所定時間経過
S２０５'
Ｙｅｓ
機能制限を再設定
S２０６'

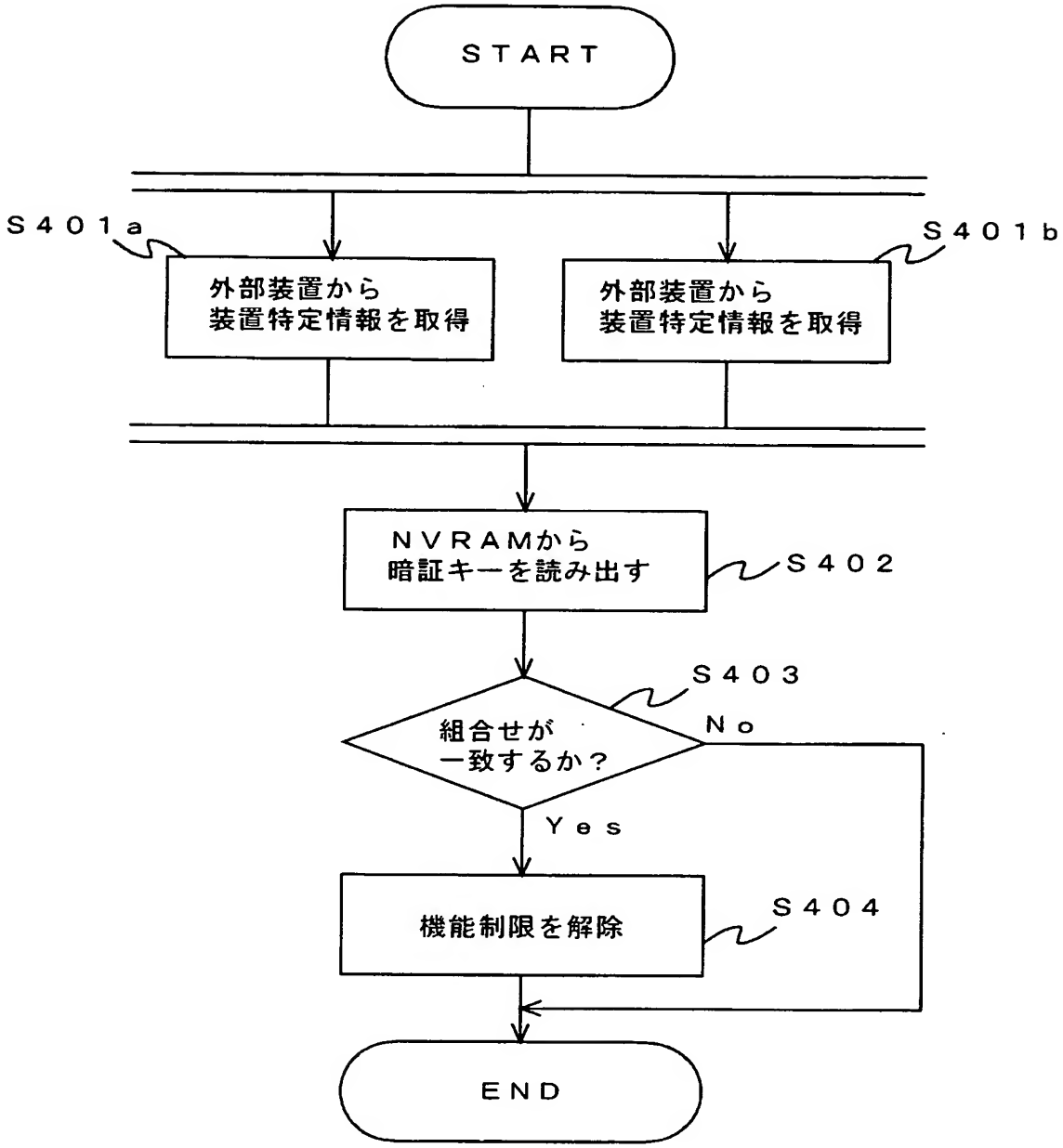
【図７】


制御部
１０１
１０４
２００
比較部
動作制限部
１０２
１０３
１０６ａ
ＮＶＲＡＭ
外部装置情報
取得部
Ｉ／Ｆ
外部装置
書込制御部
Ｉ／Ｆ
外部装置
１０５
１０７
１０６ｂ

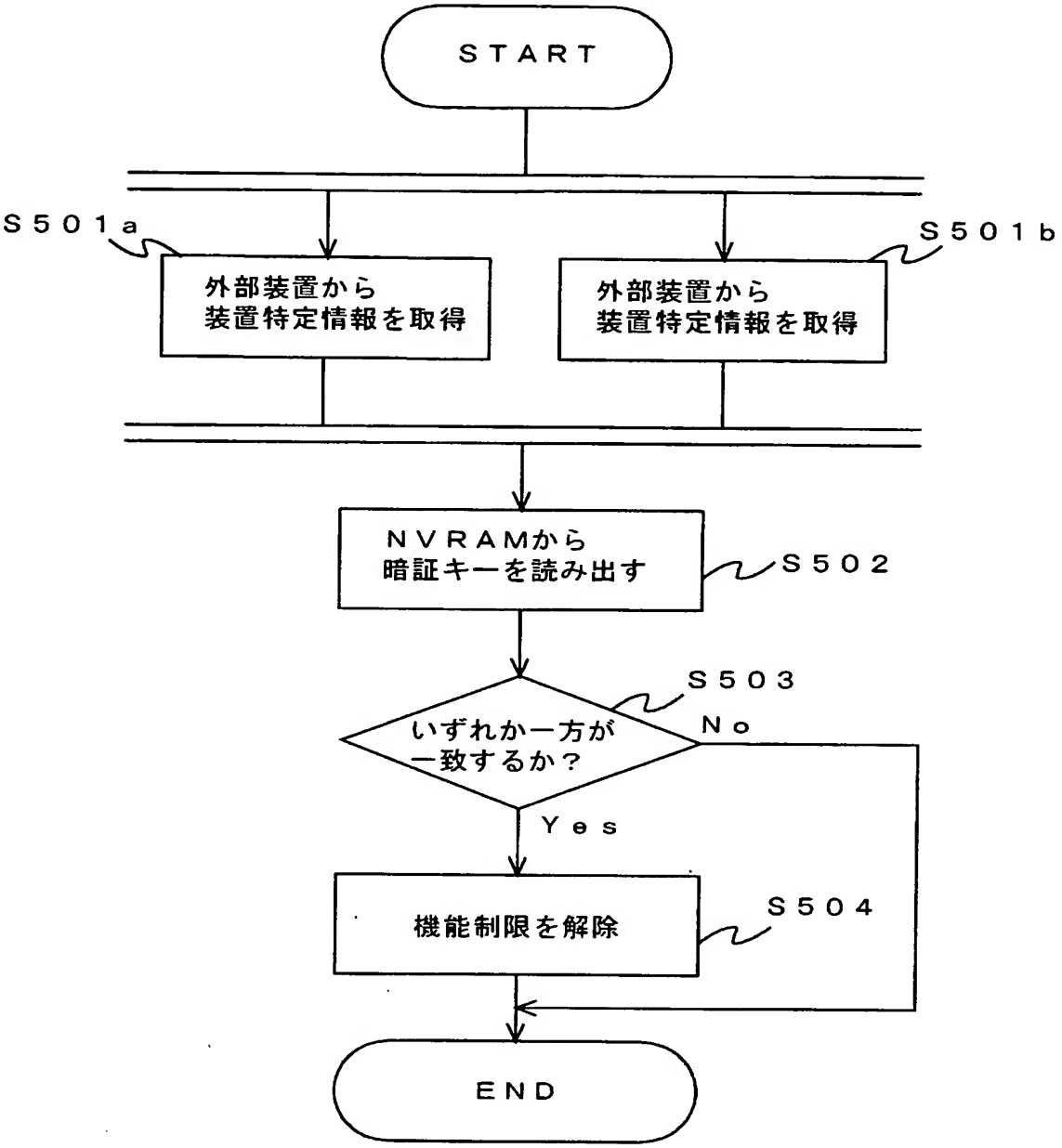
【図８】


START
S３０１a
外部装置から
装置特定情報を取得
S３０１b
外部装置から
装置特定情報を取得
S３０２a
情報記録可能な
装置か？
No
Yes
S３０２b
情報記録可能な
装置か？
No
Yes
S３０３a
装置をユニークに
示すか？
Yes
No
S３０３b
装置をユニークに
示すか？
Yes
No
S３０４a
装置をユニークに示す
情報を生成
S３０４b
装置をユニークに示す
情報を生成
S３０５a
生成した情報を
外部装置に記録させる
S３０５b
生成した情報を
外部装置に記録させる
暗証キーとして
ＮＶＲＡＭに登録
S３０６
END

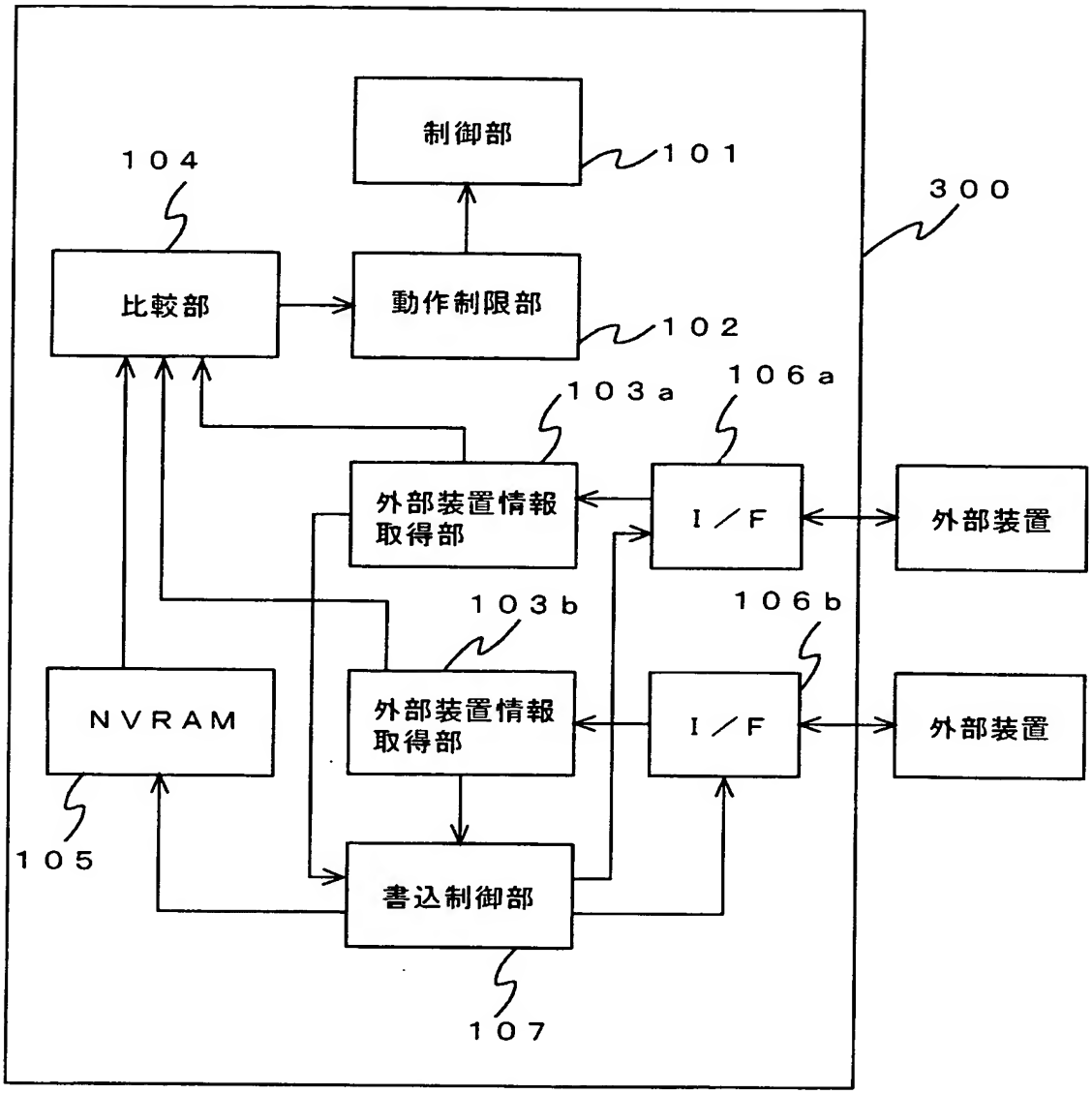
【図９】


START
S401a
外部装置から
装置特定情報を取得
S401b
外部装置から
装置特定情報を取得
NVRAMから
暗証キーを読み出す
S402
S403
組合せが
一致するか？
No
Yes
機能制限を解除
S404
END

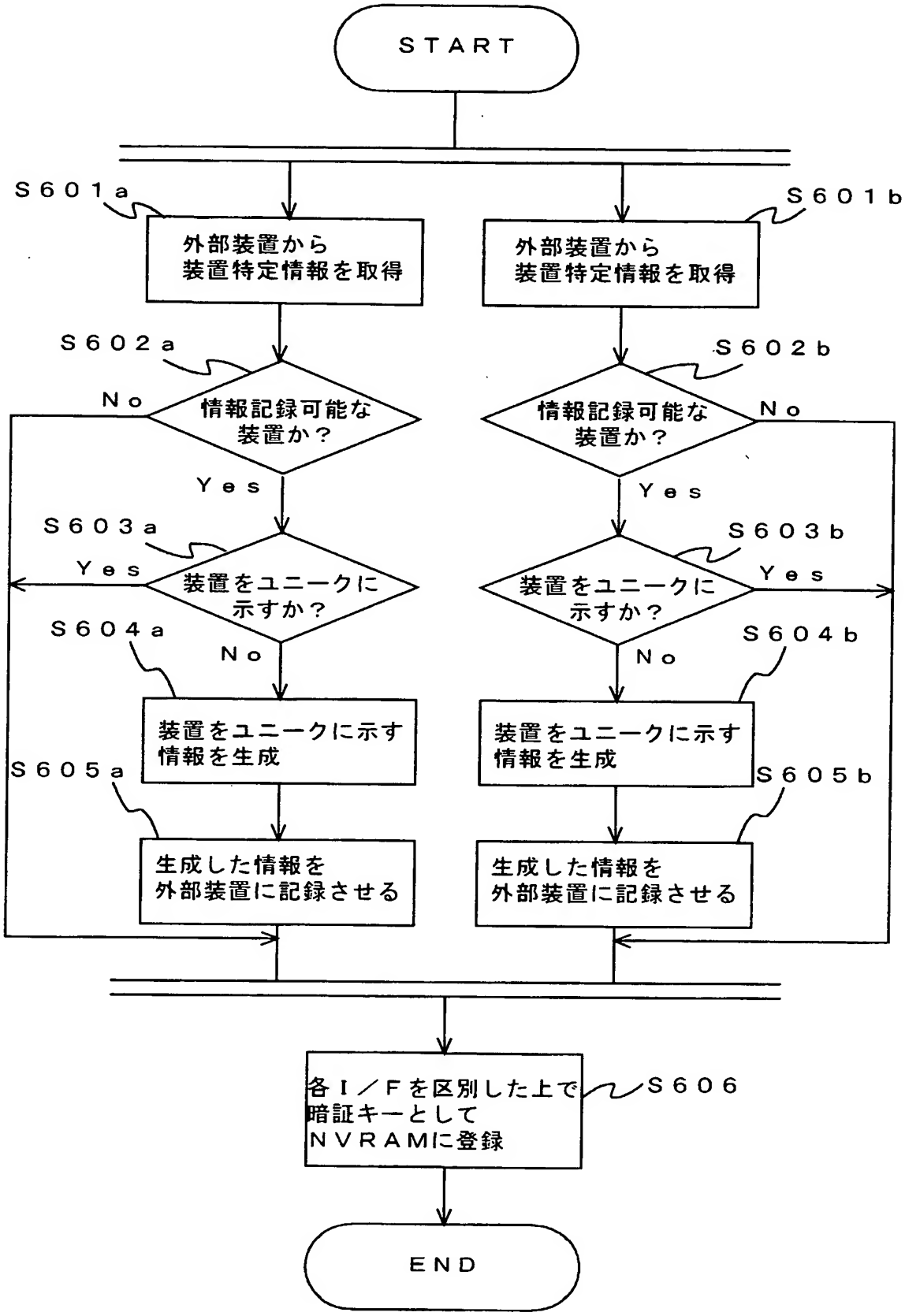
【図１０】


START
S５０１a
外部装置から
装置特定情報を取得
S５０１b
外部装置から
装置特定情報を取得
ＮＶＲＡＭから
暗証キーを読み出す
S５０２
S５０３
いずれか一方が
一致するか？
Ｎｏ
Ｙｅｓ
機能制限を解除
S５０４
END

【図１１】


制御部
１０１
１０４
３００
比較部
動作制限部
１０２
１０３ａ
１０６ａ
外部装置情報取得部
Ｉ／Ｆ
外部装置
１０３ｂ
１０６ｂ
ＮＶＲＡＭ
外部装置情報取得部
Ｉ／Ｆ
外部装置
１０５
書込制御部
１０７

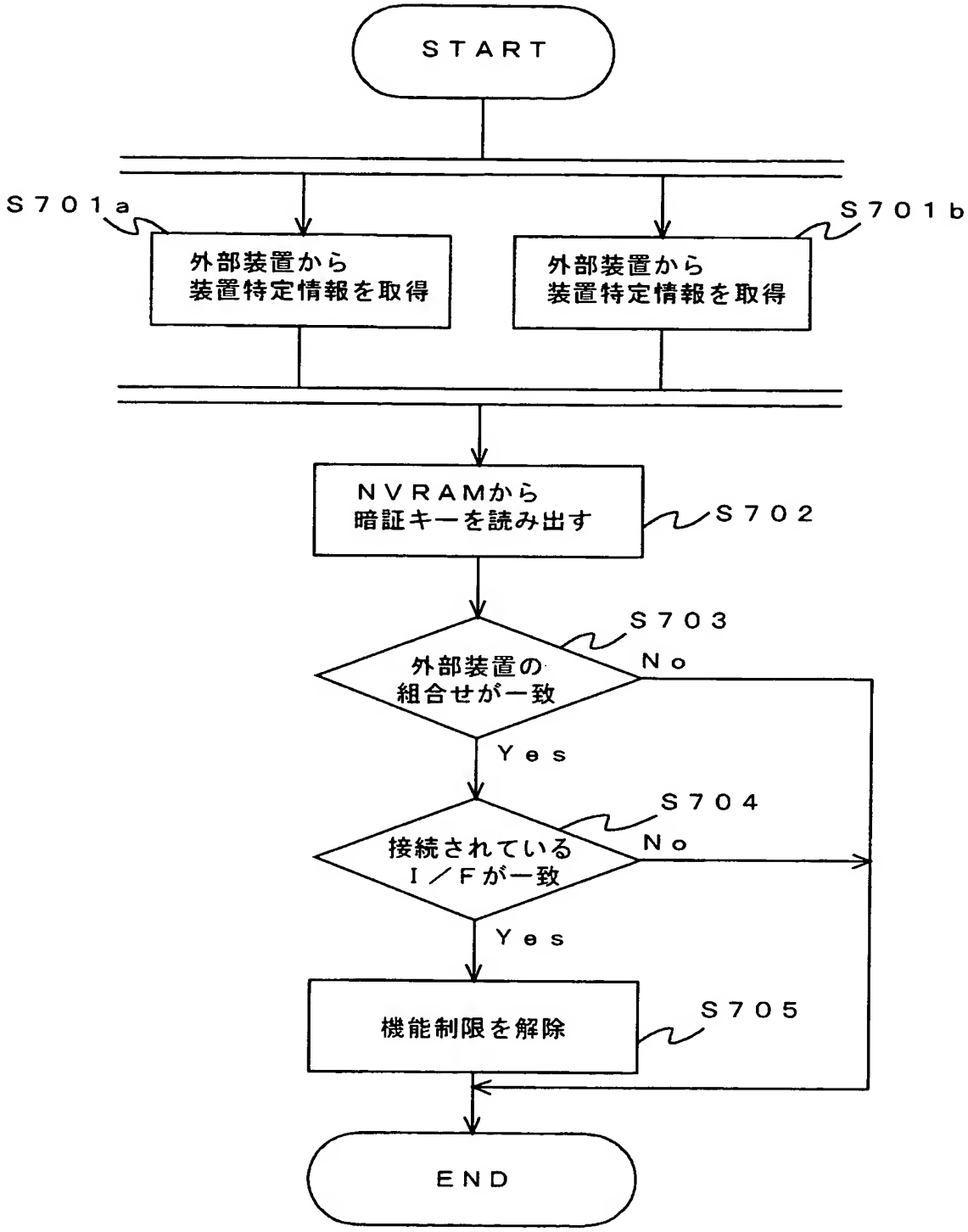
【図１２】


START
S601a
外部装置から
装置特定情報を取得
S601b
外部装置から
装置特定情報を取得
S602a
情報記録可能な
装置か？
No
Yes
S602b
情報記録可能な
装置か？
No
Yes
S603a
装置をユニークに
示すか？
Yes
No
S603b
装置をユニークに
示すか？
Yes
No
S604a
装置をユニークに示す
情報を生成
S604b
装置をユニークに示す
情報を生成
S605a
生成した情報を
外部装置に記録させる
S605b
生成した情報を
外部装置に記録させる
各Ｉ／Ｆを区別した上で
暗証キーとして
ＮＶＲＡＭに登録
S606
END

【図１３】

暗証キー	
Ｉ／Ｆ	装置特定情報
Ａ	Ｃ
Ｂ	Ｄ

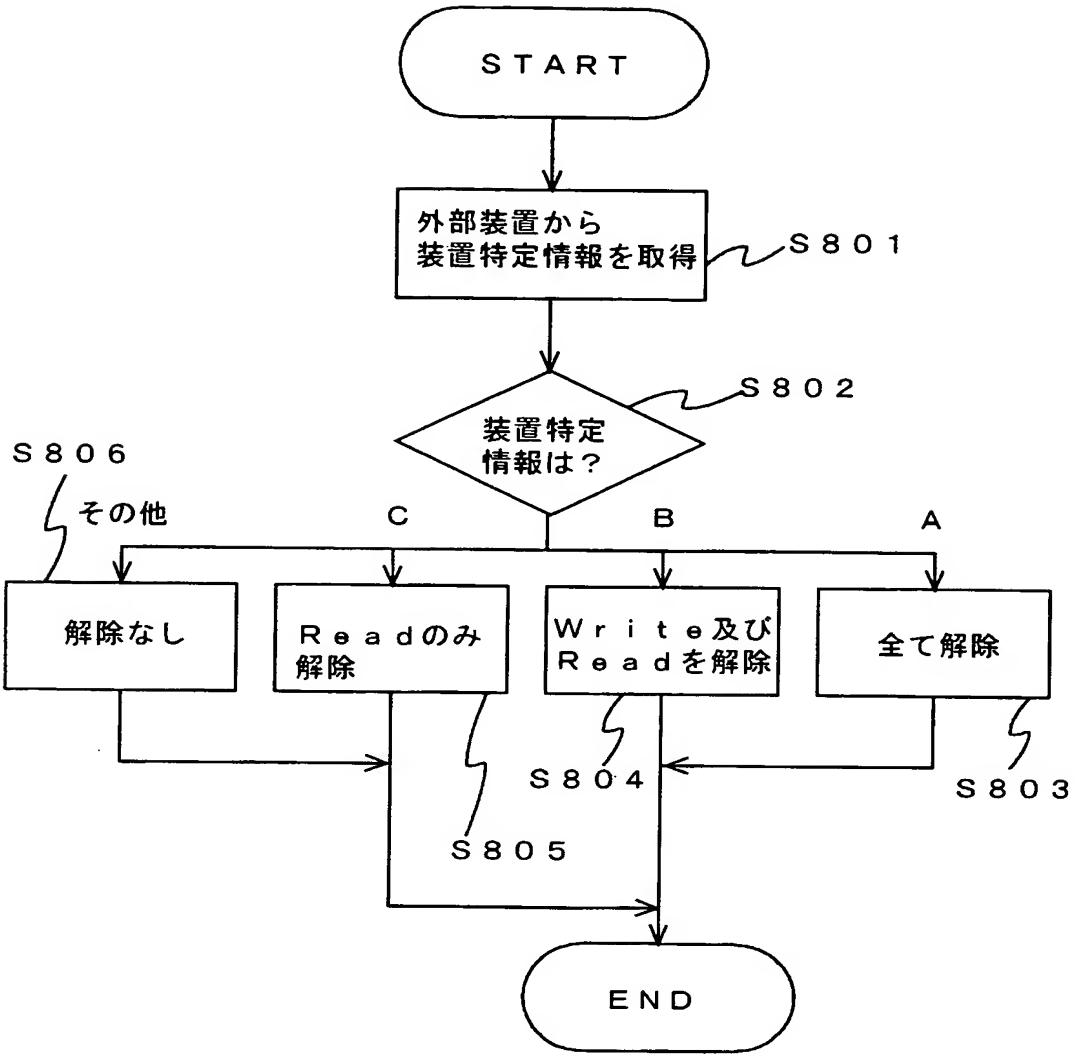
【図１４】


START
S７０１a
外部装置から
装置特定情報を取得
S７０１b
外部装置から
装置特定情報を取得
ＮＶＲＡＭから
暗証キーを読み出す
S７０２
S７０３
外部装置の
組合せが一致
No
Ｙｅｓ
S７０４
接続されている
Ｉ／Ｆが一致
No
Ｙｅｓ
機能制限を解除
S７０５
END

【図１５】

暗証キー	利用可能機能
A	All
B	Read, Write
C	Read
Default	Nothing

【図１６】


START
外部装置から
装置特定情報を取得
S８０１
S８０２
装置特定
情報は？
S８０６
その他
C
B
A
解除なし
Ｒｅａｄのみ
解除
Ｗｒｉｔｅ及び
Ｒｅａｄを解除
全て解除
S８０４
S８０３
S８０５
END

【書類名】　　要約書

【要約】

【課題】　不特定多数人が利用可能な環境に設置される電子機器の盗難を防止するとともに、電子機器に記憶された情報が盗用されることを防止する電子機器及びその不正利用防止方法並びにその不正使用防止プログラムを提供する。

【解決手段】　電子機器１００が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する動作制限部１０２と、外部装置を接続するためのＩ／Ｆ１０６と、該Ｉ／Ｆ１０６を介して接続された外部装置から該装置を特定する装置特定情報を取得する外部装置情報取得部１０３と、機能制限と所定の外部装置の装置特定情報とを関連づけて暗証キーとする書込制御部１０７と、該暗証キーを記憶するＮＶＲＡＭ１０５と、Ｉ／Ｆ１０６を介して接続されている外部装置から取得した装置特定情報が、ＮＶＲＡＭ１０５に記憶されている暗証キーと一致するか否かを判断する比較部１０４とを有し、比較部１０４が一致すると判断した場合に、動作制限部２０１が機能制限を解除する。

【選択図】　　図３

特願２００２－２３１８０６

出　願　人　履　歴　情　報

識別番号　　［３０００１６７６５］

１．変更年月日　　２００１年　４月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝五丁目３７番８号
氏　名　　エヌイーシービューテクノロジー株式会社

２．変更年月日　　２００３年　３月３１日
［変更理由］　　名称変更
住　所　　東京都港区芝五丁目３７番８号
氏　名　　ＮＥＣビューテクノロジー株式会社